

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000261751 A**

(43) Date of publication of application: **22.09.00**

(51) Int. Cl

H04N 5/765

H04N 5/781

G06F 17/60

G06K 17/00

G06K 19/07

G09C 1/00

H04N 1/387

(21) Application number: **11349816**

(22) Date of filing: **09.12.99**

(30) Priority: **17.12.98 US 98 213179**

(71) Applicant: **INTERNATL BUSINESS MACH
CORP <IBM>**

(72) Inventor: **CHAINER TIMOTHY JOSEPH
GREENGADE CLAUDE A
MOSKWECZ PAUL ANDREW
ALLENDRO GABRIEL
SUKUROTTO
CHARLES P TORRESAA
VONGUTFELD ROBERT JACOB**

**(54) SYSTEM AND METHOD FOR IMAGE
RECOGNITION**

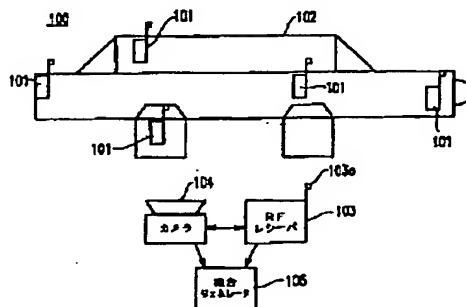
(57) Abstract:

PROBLEM TO BE SOLVED: To prevent an erroneous image from being displayed by checking at least one identifier corresponding to an object by a receiver, recording an image resulting from an object including at least one identifier, encoding an image and identification information acquired by a camera device together and generating complex data.

SOLUTION: A camera 104 acquires the image of an object to obtain a tag 101 by using the camera 104 and is connected functionally to an RF receiver 103 so as to simultaneously inquire about and read the tag 101 by the receiver 103. Further, a compound generator 105 is provided to receive inputs from both the camera 104 and the receiver 103. Especially, tag ID information from the receiver 103 is encoded along a type stamper and other information, such as the focal distance of the camera 104 and hush of a digital image acquired by

the camera 104. As a result, the generator 105 generates complex data.

COPYRIGHT: (C)2000,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-261751

(P 2 0 0 0 - 2 6 1 7 5 1 A)

(43) 公開日 平成12年9月22日 (2000.9.22)

(51) Int. Cl. ⁷	識別記号	F I	テーマコード (参考)
H04N 5/765		H04N 5/781	510 L
5/781		G06K 17/00	L
G06F 17/60			F
G06K 17/00		G09C 1/00	640 D
		H04N 1/387	

審査請求 有 請求項の数41 O L (全11頁) 最終頁に続く

(21) 出願番号	特願平11-349816	(71) 出願人	390009531 インターナショナル・ビジネス・マシーンズ・コーポレーション INTERNATIONAL BUSINESS MACHINES CORPORATION アメリカ合衆国10504、ニューヨーク州 アーモンク (番地なし)
(22) 出願日	平成11年12月9日 (1999.12.9)	(74) 代理人	100086243 弁理士 坂口 博 (外1名)
(31) 優先権主張番号	09/213179		
(32) 優先日	平成10年12月17日 (1998.12.17)		
(33) 優先権主張国	米国 (US)		

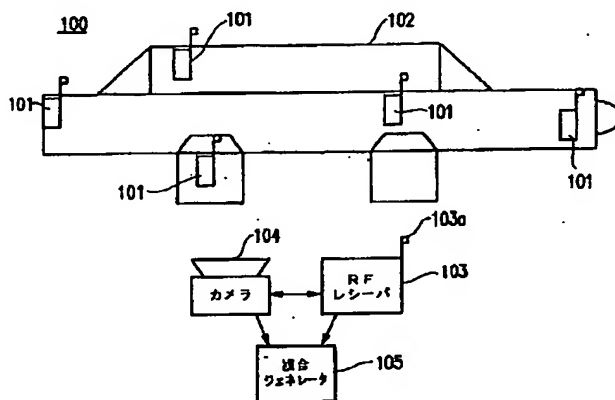
最終頁に続く

(54) 【発明の名称】 画像認証システムおよび方法

(57) 【要約】

【課題】 対象物および対象物データを確認するためのシステムおよび方法を提供。

【解決手段】 対象物の画像を認証するシステムおよび方法は、対象物に対応付けられた少なくとも一つの識別子と、少なくとも一つの識別子を問いただして識別情報を生成するレシーバと、少なくとも一つの識別子を含む対象物の画像を記録するカメラ装置と、カメラ装置によって獲得された画像に沿って、コード化されたデータとしてレシーバからの識別情報をコード化して、複合データを生成する複合ジェネレータとを有する。



【特許請求の範囲】

【請求項 1】対象物の画像を認証するシステムであって、
前記対象物に対応付けられた少なくとも一つの識別子と、
前記少なくとも一つの識別子を問いただして識別情報を生成するレシーバと、
前記少なくとも一つの識別子を含む前記対象物の画像を記録するカメラ装置と、
前記カメラ装置によって獲得された前記画像に沿って、コード化されたデータとして、前記レシーバからの前記識別情報をコード化して、複合データを生成する複合ジェネレータと、
を有することを特徴とするシステム。
【請求項 2】前記少なくとも一つの識別子は無線周波数 (RF) 識別子を有することを特徴とする請求項 1 に記載のシステム。
【請求項 3】前記少なくとも一つの識別子は生物測定的識別子を有することを特徴とする請求項 1 に記載のシステム。
【請求項 4】前記少なくとも一つの識別子はバー・コードおよびスマート・カードの少なくとも一つを有することを特徴とする請求項 1 に記載のシステム。
【請求項 5】前記レシーバは無線周波数 (RF) レシーバを有することを特徴とする請求項 1 に記載のシステム。
【請求項 6】前記少なくとも一つの識別子は前記対象物および前記対象物の特徴の少なくとも一つに特有のものであることを特徴とする請求項 1 に記載のシステム。
【請求項 7】複数の識別子が前記対象物に取り付けられていることを特徴とする請求項 1 に記載のシステム。
【請求項 8】前記コード化されたデータは、添付署名および透かしの一つとして前記画像に添付されることを特徴とする請求項 1 に記載のシステム。
【請求項 9】前記レシーバは、前記少なくとも一つの識別子とは別の識別子の読み取りを前記レシーバが行うのを妨げるために指向性アンテナを有し、該指向性アンテナは前記カメラ装置が向いている方向にある識別子のみから無線周波数 (RF) 信号を受信することを特徴とする請求項 1 に記載のシステム。
【請求項 10】前記レシーバに結合し、前記対象物に向けられた前記レシーバのパルスの開始と前記レシーバによる前記パルスの受信との間の遅延時間を測定する遅延感知サブシステムを、さらに有することを特徴とする請求項 1 に記載のシステム。
【請求項 11】前記識別情報は、前記カメラ装置と前記対象物との距離と、前記カメラの焦点距離との少なくとも一つを含むことを特徴とする請求項 1 に記載のシステム。
【請求項 12】請求項 1 に記載のシステムであって、前

記複合ジェネレータに結合した暗号化装置をさらに有し、前記少なくとも一つの識別子と所定の情報とからの識別情報のコード化は、公開鍵および秘密鍵の一つを用いる前記複合ジェネレータから前記暗号化装置への入力であることを特徴とする請求項 1 に記載のシステム。
【請求項 13】前記カメラ装置は、ズーム・レンズ系を有し、前記ズーム・レンズ系の複数の異なるズーム設定によって複数の画像を自動的に形成することを特徴とする請求項 1 に記載のシステム。
【請求項 14】前記レシーバは該レシーバに取り付けられた識別子を有し、前記対象物の画像を前記カメラ装置が撮る際に前記レシーバの前記識別子と前記対象物の前記少なくとも一つの識別子との両方が記録されることを特徴とする請求項 1 に記載のシステム。
【請求項 15】前記少なくとも一つの識別子に対応する署名は、事前に記録されていることを特徴とする請求項 1 に記載のシステム。
【請求項 16】前記少なくとも一つの識別子は、無線周波数識別タグを有することを特徴とする請求項 1 に記載のシステム。
【請求項 17】前記画像はタイム・スタンプによりコード化されていることを特徴とする請求項 1 に記載のシステム。
【請求項 18】前記画像にタイム・スタンプを暗号化するための手段をさらに有し、前記タイム・スタンプは前記画像が前記カメラ装置によって記録された時間を表示することを特徴とする請求項 1 に記載のシステム。
【請求項 19】前記画像が前記カメラ装置によって記録された時間を感知する手段と、
前記画像にタイム・スタンプを埋め込む手段と、
前記タイム・スタンプを含む前記画像を暗号化する手段と、
をさらに有することを特徴とする請求項 1 に記載のシステム。
【請求項 20】前記少なくとも一つの識別子は、前記少なくとも一つの識別子の変化あるいは除去のいずれの場合も前記少なくとも一つの識別子を無効にするように、耐改ざん識別子を有することを特徴とする請求項 1 に記載のシステム。
【請求項 21】対象物を認証する方法であって、対象物に少なくとも一つの識別子に対応づける工程と、前記少なくとも一つの識別子を問いただすことで識別情報を生成する工程と、
前記少なくとも一つの識別子を含む前記対象物の画像を記録する工程と、
複合データを生成するために、記録された前記画像に沿って、前記少なくとも一つの識別子に対する前記問いただしにもとづいて、前記識別情報をコード化する工程と、
を有することを特徴する方法。
【請求項 22】前記少なくとも一つの識別子は無線周波

数識別子を有することと特徴とする請求項 2 1 に記載の方法。

【請求項 2 3】前記少なくとも一つの識別子は生物測定的識別子を有することを特徴とする請求項 2 1 に記載の方法。

【請求項 2 4】前記少なくとも一つの識別子はバー・コードおよびスマート・カードの少なくとも一つを有することを特徴とする請求項 2 1 に記載の方法。

【請求項 2 5】前記少なくとも一つの識別子は前記対象物および前記対象物の特徴の少なくとも一つに特有のものであることを特徴とする請求項 2 1 に記載の方法。

【請求項 2 6】前記少なくとも一つの識別子は、耐改ざん識別子を有し、前記少なくとも一つの識別子の変化および除去のいずれの場合に対しても応答する前記耐改ざん識別子を無効にする工程をさらに有することを特徴とする請求項 2 1 に記載の方法。

【請求項 2 7】対象物を認証する方法であって、前記対象物に対応した少なくとも 2 種類の情報を同時に抽出する工程と、前記抽出とともに、同時に前記少なくとも 2 種類の情報を一緒に暗号化する工程と、前記少なくとも 2 種類の情報を解読し、前記対象物の認証を確かめる工程と、を有することを特徴とする方法。

【請求項 2 8】前記抽出する工程は、前記対象物の画像を記録する準工程と、前記対象物の固有の物理的特性を得る準工程とを有することを特徴とする請求項 2 7 に記載の方法。

【請求項 2 9】前記画像は写真画像を有し、また前記固有の物理的特性は前記対象物の表面の地形学的測定を含むことを特徴とする請求項 2 8 に記載の方法。

【請求項 3 0】前記画像は写真画像を有し、また前記固有の物理的特性は前記対象物の密度および重量の少なくとも一つを含むことを特徴とする請求項 2 8 に記載の方法。

【請求項 3 1】前記密度は前記対象物の立体的空隙を明らかにすることを特徴とする請求項 3 0 に記載の方法。

【請求項 3 2】前記画像は写真画像を有し、また前記少なくとも一つの固有の特性は前記対象物の磁性的特性をふくむことを特徴とする請求項 2 8 に記載の方法。

【請求項 3 3】前記 2 種類の情報の一つは前記対象物の電磁気照射を有することを特徴とする請求項 2 7 に記載の方法。

【請求項 3 4】前記 2 種類の情報の一つは、識別する情報を発する電子タグの一つから、および外部フィールドによって促された場合に前記 2 通りの情報の一つを明らかにする受動的タグからのものであることを特徴とする請求項 2 7 に記載の方法。

【請求項 3 5】前記 2 通りの情報の少なくとも一つは、

時間順の順序で適応されることを特徴とする請求項 2 7 に記載の方法。

【請求項 3 6】前記 2 通りの情報の少なくとも一つは、前記対象物のデジタル画像を有し、前記対象物は立体状の対象物を有することを特徴とする請求項 2 7 に記載の方法。

【請求項 3 7】前記 2 通りの情報は、前記対象物の画像情報と前記対象物に固有に対応付けされた生物測定的情報とが含まれることを特徴とする請求項 2 7 に記載の方法。

【請求項 3 8】前記 2 通りの情報は、前記対象物に対応付けされた無線周波数 (R F) タグであることを特徴とする請求項 2 7 に記載の方法。

【請求項 3 9】前記 2 通りの情報は、前記対象物に対応付けされた生物測定的識別子であることを特徴とする請求項 2 7 に記載の方法。

【請求項 4 0】前記 2 通りの情報の一つは、前記対象物に対応付けられたバー・コードおよびスマート・カードの少なくとも一つからのものであることを特徴とする請求項 2 7 に記載の方法。

【請求項 4 1】前記 2 通りの情報の一つは、前記対象物に対応づけられた少なくとも一つの識別子からのものであり、前記少なくとも一つの識別子は耐改ざん識別子を有し、前記少なくとも一つの識別子の変化あるいは除去のいずれの場合にも応答して耐改ざん識別子を無効にする工程をさらに有することを特徴とする請求項 2 7 に記載のシステム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】本発明は、一般に画像認証システムおよび方法に関する。

【 0 0 0 2 】

【従来の技術】無生物からなる対象物および生物からなる対象物の両方の誤りを立証する多くの試みがなされている。保険会社が直面する特に重要な問題の一つとして、特に限られるわけではないがモータによって駆動する乗り物 (motor vehicles) (自動車、トラック、バイク等) に対する損害または修復状態の改ざんがある。

【 0 0 0 3 】多くの場合、事故が起こると事故車は修理工場または自動車販売店に運ばれ、損害の程度が写真に撮られる。その後、修理したと言われた後に 2 枚目の写真が撮られる。続いて、費用を回収するために 2 枚目の写真が保険会社に提出される。しかし、しばしば 2 枚目の写真 (あるいは 1 枚目および 2 枚目の写真両方) が改変 (例えば、変造) されたり、あるいは別の車両の写真が使われたりする場合がある。

【 0 0 0 4 】したがって、悪辣きわまる修理店および (または) 自動車のオーナーの手にかかって保険会社に対する詐欺的な不法行為が生ずる。

【0005】さらに、従来のシステムのなかには、提示すべきと思われる対象ではないものの写真を撮ることを防止するための方法（あるいは少なくともそれを発見するための方法）が存在しないものがある。

【0006】例えば、修理が実際には行われてないのに修理費を得るために、事故にあった車と外観は類似しているが形状は完全である車（損害を受けていない車等）の画像を記録し、その画像を保険会社に送ることを発見する方法はない。

【0007】上記問題を解決するには、カメラによって撮られた画像が信頼できる画像となることが必要である。一従来システムでは、デジタル署名をコード化し、それをデジタル・カメラによって獲得した画像に添付することによって画像の認証を行う装置が提供されている。

【0008】そのようなシステムでは、デジタル・カメラは生成した画像を認証する署名を創出する暗号化技術を利用する。特に、コード化されたメッセージを画像に添付することで認証を可能とする。他の情報も画像に添付することができる。しかし、そのようなデジタル・カメラを含む従来のシステムは、不正行為のすべての形態を確実に防ぐ（あるいは少なくとも検出する）ことができない。例えば、従来のシステムは、以下に記述する不正行為を防ぐことはできないだろう。

【0009】第1に、デジタル・カメラに呈示された画像が写真であり、対象物（例えば、車）の状態の実際の画像が不必要な場合がある。

【0010】第2に、温度等、画像に添付された追加情報が他のソース由来で、様々なタイプのリレーや中間デバイス／ノードを経由してデジタル・カメラの記録場所から生じたように表される。したがって、たとえ従来のシステムが不正変更等の上記した問題のいくつかを克服したとしても、なおも解決すべき課題が存在する。例えば、そのようなシステムは、大量生産によって得られる品物（例えば、テレビ、ビデオ・テープ・レコード等の家庭用電子機器、自動車、オートバイ、ボート等のモータによって駆動する乗り物、工芸品、高価な衣類等）等の外見が似通った品物同士を区別することはできない。

【0011】したがって、不正行為を確実に防ぐことができず、それによって保険会社（さらに最終的には合法的な策を取る者）は年に何億ドルもの出費が強いられる。

【0012】

【発明が解決しようとする課題】従来のシステムおよび方法の上記した問題や他の問題を鑑みて、本発明の目的は誤った画像の表示を防ぐための方法およびシステム、特に、例えば後に行われる修理を誤って表示することと同様に損害の誤った表示を防ぐ方法およびシステムを提供することである。

【0013】本発明の別の目的は、カメラとリーダ（例

例えば、無線周波数（RF）リーダ）とを併用する構造および方法を提供することを目的とする。リーダは、対象物の画像と、該対象物の識別に対応し、かつその対象物に対応付けられた少なくとも一つのタグに割り当てられた一連のビットとの両方を同時に記録する。

【0014】本発明のさらに別の目的は、対象物に関する複数の種類の情報を用い、それを安全確実な方法でもって保存することによって、実際の対象物に対応付けられると主張するデータを認証するシステムおよび方法を提供することを目的とする。このシステムおよび方法は、デジタル画像の認証を提供するために写真と組み合わせ使用される。

【0015】

【課題を解決するための手段】本発明の第1の態様では、対象物の画像を認証するシステムは、対象物に対応付けられた少なくとも一つの識別子と、この少なくとも一つの識別子を取り調べるためのレシーバと、少なくとも一つの識別子を含む対象物由来の画像を記録するためのカメラ装置と、カメラ装置およびレシーバからの入力を受け取るための複合ジェネレータとを有し、レシーバからの識別情報はカメラ装置によって獲得された画像と一緒にコード化され、複合ジェネレータによって複合データが生成される。

【0016】本発明のもっとも単純な構成では、従来のシステムおよび方法の上記問題は、タグを破壊しないかぎりタグを除去することができないようにして対象物に対応付けられた一つ以上のタグ（例えば、無線周波数（RF）タグ、磁気タグ、スマート・カード、バー・コード、生物測定学的（バイオメトリック）識別子等）を有する新規なシステムによって克服する。各々のタグには、異なるIDまたは特有のIDが与えられている。

【0017】自動車の修理に関わる実施形態例について再び説明する。典型的な自動車事故の際に少なくとも一つのタグが残るよう、好ましくは自動車の互いに異なる位置にいくつかのタグが取り付けられている。

【0018】自動車の損害を査定する場合、複合光学無線周波数識別（RFID）写真が撮られる。そのような写真を撮る場合、カメラの焦点を自動車の損害部分に合わせる。好ましくは各損害部位はタグを有するので、光学写真を撮ると、写真上に認証を目的とした「透かし模様」が置かれるので、IDを読み取ることができる。修理後、光学RFID写真を同一カメラ／RFリーダで撮影し、さらにこの写真をオリジナル写真とともに保険会社に提出して、これらの写真（およびタグ上の光学署名）を比較する。

【0019】さらに、注目すべき点はタイム・スタンプを付与する装置および（または）距離を判断する装置もまた設けることが可能であるということである。例えば、レンジファインダで使用されるような光ビームを距離を測定するために用いてもよい。あるいは、カメラか

ら対象とする対象物までの距離を測定するために音響センサを用いることができる。そのような距離測定機能によって、より高い信頼性が得られ、さらに実際の対象物に対して多くの場合遠く離れて位置した不正な画像を撮るためのリレー等の確立を阻止する役割を果たす。

【0020】さらに、本発明は、対象物、場合によってはその環境（例えば、画像および温度）の少なくとも2つの特性の抽出と、一緒にこれらの抽出された結果をプライベート・キーを用いて一つにまとめられたデータ・セットに暗号化することを同時に行うことで、対象物に関する情報を認証する。遠隔地にいるこの情報のユーザは、暗号化された情報を公開または秘密鍵暗号解読によって入手可能とすることができる。

【0021】上記したように、例えば対象物の写真は該対象物についてのいくつかの情報を遠隔側に提供しますが、透かし模様による写真の認証があるにもかかわらず、そのような情報は認証できるものでないかもしれない。なぜなら、写真は対象物そのものではなく該対象物を不正なかたちで撮ったもの、あるいはコンピュータ画面上から撮ったものであるかもしれないからである。写真の画像を別の認識可能なものと組み合わせることで、かなり強化された認証が可能である。このことはビデオカメラで撮られた画像にも同様に適用される。さらに、情報の最初の出所は視覚化される必要はないので、本発明はどのような記録の信用でも高める。

【0022】対象物の特性の一つは、タグによって確認されるような個性である。対象物に組み入れられあるいは取り付けられた識別タグからの広範囲な識別情報を他の検出された情報と同時に検出（および暗号化）することで、測定されたデータと特異的に識別された対象物との間の信頼度をよりいっそう高くすることができる。

【0023】さらに、本発明は物理的対象物から抽出されたと申し立てられたデータと対象物それ自体のデータとの相互関係を認証するために脆い透かし模様を使用することができる。この発明は、物理的対象物についての情報のユーザが該物理的対象物についての情報の信憑性についてより高い信頼性を得ることを可能とする。本発明は、好ましくは同時に生成されたいくつかのデータ・セットの不正な透かし模様を使用する。公開または専用暗号鍵、またはそれらの組み合わせを用いて検証プロセスを実施することができる。

【0024】

【発明の実施の形態】以下、図面を参照しながら、本発明にもとづくシステムを説明する。図1は、本発明の好ましい一実施形態例にもとづくシステム100を示す。

【0025】図に示すように、システム100は対象物102に対応付けられた（例えば、取り付け、支持、設置等）少なくとも一つのタグ101を有する。いっそう好ましくは、さらに大きな信頼性を得るために複数のタグ101が対象物に対応付けられる。好ましくは、タグ

は無線による無線周波数識別（RFID）タグであり、周囲にさらされ、かつタグから画像を得るようなかたちで画像形成装置によって可視化される。タグは情報によってコード化されており、該タグが取り付けられた車を特異的に識別する役割を果たす。上記したように、タグを変え、さらに（あるいは）それを別の車に取り付けようとする試みはいずれの場合もタグを破壊または使用不可能な状態にする（例えば、タグを無効にする）。

【0026】したがって、タグを対象物に対応付けたり、取り付けたり、保持させたり、あるいは組み込んだりすることができる。タグは注文制作されたものでもよく、あるいはBradyらの米国特許第5,682,143号、Welshらの米国特許第4,063,229号、Slobodinの米国特許第4,242,663号およびMawhinneyの米国特許第4,646,090号等の多くの参考文献（これらの文献の記載を本明細書の記載の一部として援用）のいずれかに記載された同様の、あるいは類似したタグであってもよい。さらに、タグは数多くある製造元（Motorola、Texas Instruments等）のいずれかから市販されている。さらに別の種類のタグを上記したタグと一緒に、あるいはその代替品として用いてもよい。そのような別の種類のタグとしては、「無線周波数自動識別システム」と題されたGreeneらの米国特許第5,581,257号（この文献の記載を本明細書の記載の一部として援用）に開示されたRFタグや磁気タグがあげられる。さらに、別の応用としては、スマート・カード、バー・コード、バイオメトリック識別子があげられる。以下に例示する実施形態例では、便宜上、タグはRFIDタグであるとして説明する。

【0027】RFIDタグ101に対する問い合わせ／読み取りを行うために、アンテナ103aを備えるレシーバ／タグ・リーダ103（例えば、無線周波数（RF）レシーバ／タグ・リーダ）が設けられている。

【0028】また、タグ101を有する対象物102の画像を記録するために、カメラ装置104（例えば、電荷結合素子（CCD）等のデジタル・カメラ）が設けられている。このカメラ104は、タグを有する目的とする対象物の画像をカメラ104が取得し、RFレシーバ103によってタグに対する問い合わせおよび読み取りを同時に行うように、カメラ104がRFレシーバ103と機能的につながっている。

【0029】さらに、カメラ104およびタグ・リーダ103の両方からの入力を受信するために、複合ジェネレータ105が設けられている。

【0030】特に、RFリーダ103からのタグID情報は、タイプ・スタンプ（例えば、問い合わせパルス出力の時間、タグからの問い合わせ情報受信の時間）や、他の情報、例えばカメラ104の焦点距離、カメラ104によって取得されたデジタル画像のハッシュ（例えば、場合によっては暗号化または非暗号化されたもの）に沿ってコード化される。

【0031】その結果、複合ジェネレータ105は複合データを生成する。

【0032】コード化されたデータは、例えば米国特許第5,499,294号（この文献の記載を本明細書の記載の一部として援用）に開示されているような添付署名として、あるいは「壊れやすい透かし模様」として添付することができる。

【0033】感知できないほどの透かし模様は、人がかろうじて認知できる程度、あるいはまったく認知することができないけれどもコンピュータ等の機器によって認知可能なデータ・セットの改ざんである。コンピュータ以外では、透かし模様は本質的に不可視とすべきである。そのような透かし模様の一般原理は、例えばM. M. Y eungらの「高品質画像のためのデジタル透かし模様形成 (Digital Watermarking for High-quality Imaging)」、Proceedings of the IEEE Signal Processing Society Multimedia Workshop, Princeton, New Jersey 1997に開示されている。壊れやすい透かし模様（例えば、画像が信用できるもので改ざんされていないことをユーザが認知できる透かし模様）を使用することができる。透かし模様を用いるかわりに、例えばFriedmanの米国特許第5,499,294号（この文献の記載を本明細書の記載の一部として援用）および上記したように、画像に認証メッセージを添付することもできる。

【0034】対象物102に取り付けられていないタグの読み取りをRFリーダ103がしないようにするために、RFリーダのアンテナは好ましくは指向性アンテナであり、またアンテナ/RFレシーバはデジタル・カメラ104と結合して移動する。したがって、指向性アンテナは好ましくは光学カメラが向けられた方向のみのRF信号を受信し、それによって光学画像データとRFデータとの両方が同一位置から作り出されることが確認される。

【0035】図1に示したような第1の好ましい実施形態例のほかに、本発明の精神および範囲内で以下のような変更が可能である。理解を容易にするために、図2はシステム100に以下のような変更を加えたシステム200の構成を説明するためのブロック図である。そのような変更は図1に示す基本的構成に対して任意に行われるものなので、変更に該当する部分は破線で示す。さらに、より多くの利点をえるために以下の変更が単独であるいは組み合わせて用いてもよい。

【0036】例えば、タグ101、RFレシーバ103、カメラ104および複合ジェネレータ105のほかに、システム200はRFリーダパルスの開始と該パルスの受信（例えば、タグ・リーダ103によって）との間の遅延時間を測定するための装置106（例えば、遅延センサまたは遅延感知サブシステム106）を含むものであってもよい。この形式では、RFリレー・ステーションがシステムの回避や不正な画像の提供に利用され

ているかどうか感知できる。

【0037】特に、電磁波の速度が 3×10^8 m/秒なので、修理された車を包含する画像はカメラと画像との離間距離が約3~5 mのオーダーであることを要求するだろう。この距離は光学カメラ104の焦点距離を測定することによって測定することができる。したがって、開始信号に対する遅延は約20~33ナノ秒のオーダーであろう。いずれの時間も、リレー・セットアップが他の位置からのRF信号をリレーするのに使用されることを示す時間と著しく異なる（例えば、その時間よりも長い）。遅延時間は、好ましくは複合ジェネレータ105によって記録され、かつコード化されて複合データとなる。遅延センサ106は、以下に説明するタイム・スタンプ・センサ/暗号化装置109によって有利に用いることができる。

【0038】図1に示す好ましい実施形態例に対する別の変形例では、例えばFriedmanの米国特許第5,499,294号公報に記載されているように、公開鍵または秘密鍵暗号文のいずれかをを用いて、RFタグからのデータおよび別の情報のコード化を複合ジェネレータ105から暗号化装置107に入力してもよい。

【0039】したがって、コード化されたデータは公開鍵暗号文または秘密鍵暗号文のいずれかをを用いてさらに暗号化される。いずれの場合も、周知のごとく、コード化データを解読するために適当な解読鍵が必要である。

【0040】具体例としての暗号化のためのシステム300を図3に示す。この図において、対象物の写真画像302および対象物の事前選択された特性304と秘密鍵情報とが暗号化装置308に入力される。そして次に暗号化装置304は認証のための暗号化された画像310を生成する。特定の暗号技術（例えば、SK/PK対およびハッシュ機能）についての説明は、Alfred J. MenezesらのHandbook of Applied Cryptography (CRC Press, 1997)に記載されている。

【0041】図3において、対象物のデジタル画像は図1のデジタル・カメラ装置104または標準的な写真材料によって記録された表面のフォトンの反射を表す。この画像は、対象物の現在の状態を示し、またしばしば証拠として使用される。例えば、上記したように、自動車の事故による損害の写真を保険支払請求の証拠として使用してもよい。画像の操作は可能である。

【0042】したがって、図3において、立体的な対象物が詳細に検討され、画像302および対象物の特性304を含む少なくとも2つのデータ・セットが図3に示すように暗号化装置306によって一緒に暗号化される。例えば、これはカメラで撮影した対象物の画像および干渉（例えば、電磁波または音波のいずれかによる）測定値であってよい。複合データ・セット310は、このデータ・セットが実際の対象物を表していること、またシミュレートされた対象物あるいは画面上またはい

ずれかの他の平面的な媒体を写真に撮った後の対象物の画像を操作したものではないことを認証する。

【0043】図4では、そのような情報を提供する一例が図示されている。対象物406はワイン・ボトルである。このワイン・ボトルをデジタル・カメラ400によって撮影してもよい。写真が実際に目的とする立体的な対象物の画像であることを確かめるために、対象物からの距離および（または）対象物の寸法の測定に距離および（または）寸法測定装置400が用いられる。そのような装置は、カメラから発してエコーが実質的に画像を取り込む時にカメラによって受け取られる電磁波および（または）音波を使うものであってもよい。さらに、ワイン・ボトルは電子タグ408を有し、またこの情報がRFIDタグ・リーダ410にも送られ、またカメラ400によって記録される。対象物を表現するために、図3に示すとおりにすべての情報がひとまとめにされて暗号化される。

【0044】図4に示す例では距離のみが用いられているが、対象物の多くの態様および特性を記録することができよう。例えば、限定されるものではないが、重量、対象物の立体的空隙を示す密度、振動準位、核磁気共鳴（NMR）、赤外線スペクトル、電磁波放射等があげられる。

【0045】再び図2を参照しながら説明する。図1の基本システムの別の変形例は、ズーム・レンズ108を有するカメラ104と設けることと複数の異なるズーム設定（例えば、好ましくは無作為に設定）で複数の写真を自動的に撮ることとが含まれる。ズーム設定は一つの、あるいは両方の画像に対してコード化される。

【0046】別の変形例では、上記のシステムにおいてリーダにもRFタグ101が含まれており、リーダのRFタグと対象物102のタグとが画像撮影の際に記録される。この組み合わせは不正行為の目的でリーダ103とカメラ104とをエミュレートするのをよりいっそう困難にさせる。さらに、さらにいっそう高い信頼性および安全性を得るために、タグを付けたデジタル・カメラを写真撮る特定の修理店／法人に登録することができよう。

【0047】システムのさらに別の変形例では、シリコン技術よりはむしろ様々な双極子を持ち、かつアナログ様式で読み取られる少なくとも一つのタグ501（およびより好ましくは複数のタグ501）を提供することが含まれる。そのようなタグの一つの具体化されたものが「無線周波数自動識別システム」と題されたGreeneらの米国特許第5,581,257号（この文献の記載を本明細書の記載の一部として援用）に記述されている。そのようなタグ501では、ワイヤ502が例えば紙製のパッケージング／ハウジング503（例えば、紙「マッシュ」またはパルプ）のなかでランダムに分布している。そのようなタグを、該タグを単純に読み取るだけでは複製する

ことができない。それらのタグに対応する署名を事前に記録し、データベース（例えば、保険会社等で）に保存しておく。タグの署名は無線周波数を用いることで記録されるが、典型的なシリコンRFIDタグとは異なる様式で読み取られる。ランダムに配列されているので、もしワイヤの分布の構成が変化したらなば、事前に記録した信号を複製することはできない。

【0048】さらに別の変形例では、タイム・スタンプを感知して暗号化する装置109が設けられる。すなわち、この装置109はカメラ装置によって記録された画像上のタイム・スタンプを感知して暗号化するためのものである。タイム・スタンプは、カメラによって画像が記録された際の時間を表し、画像に対する認証の別のレベルを提供するであろう。

【0049】したがって、本発明は、例えば保険の目的で表現されたと思われる実際の対象物とは異なる対象物の写真を撮る不正行為を抑止する。そのような不正行為をかなり高い信頼性をもって検出するので抑止力となる。例えば、本発明によって可能となった高い信頼性を持つ検出によって、事故に遭った自動車に外観が類似した無傷の車の画像を記録し、修理が実際に行われていない（またはある場合においては修理を必要としない）場合に、支払い請求のために保険会社にそのような画像を送るという不正行為が抑止されるであろう。

【0050】さらに、本発明は誤りの、あるいは偽造の遠隔画像を送ることが可能なリレー・ステーションの設定を抑制またはごく少なくとも思いとどまらせる。

【0051】本発明を好ましい実施形態の面で説明してきたが、本発明の特許請求の範囲の目的および範囲から逸脱することなく変更を加えて実施することが可能であることは当業者ならば容易に理解されよう。

【0052】例えば、測定機器（例えば、「検知器（sniffer）」または音響装置等）がタグを備えるでる限り、臭いとか音とかの他のパラメータを測定することができよう。パラメータの表示を信頼性および確実性を得るために写真上に置くことができよう。

【0053】さらに、上記したタイム・スタンプは米国連邦標準局（NBS）から発せられる国内無線局報時信号（例えば、無線局呼び出し符号「WWV」）あるいはインターネットのウェブ（WWW）上で調整されるものであってもよい。高い信頼性を有する認証のために、目的とする対象物の写真または画像の中にそのような時間を暗号化することができよう。

【0054】さらに、上記のタグは外部フィールドによって質問されるタグとして記述されてきた。識別情報を発するために受動的タグに加えて、あるいはその代わりとして「アクティブ」電子タグを用いることもできよう。

【0055】さらに、自動車を扱った具体例、非限定的実施形態および変形例を説明してきたが本発明は大量生

産される家庭用電化製品、例えばテレビ、ビデオ・テープ・レコーダ等や、トラック、バイクおよびボート等の他のモータ駆動の乗物や、航空機、工芸品、高価な衣類等の他の対象物にも等しく適用可能である。したがって、無生物の対象物は本発明によって多大な利益を見いだすであろう。

【0056】さらに、本発明のシステムは、生命を持つ対象物（例えば、人、動物等）の識別にも容易に利用することができよう。そのような場合、生命のある対象物の写真を撮る（例えば、画像を得ること）一方で、同時に他のデータ（例えば、虹彩／網膜の形状、歯形等の生物測定的情報を確認する）を得ることで、生命ある対象物を識別することができる。さらに生命ある対象物はタグ（例えば、無線周波数（RF）タグ、磁気タグ、スマート・カード、バー・コード、生物測定的識別子等）を運ぶことが可能である。したがって、無生物および生物からなる対象物を本発明によって容易に認証することができる。

【0057】まとめとして、本発明の構成に関して以下の事項を開示する。

(1) 対象物の画像を認証するシステムであって、前記対象物に対応付けられた少なくとも一つの識別子と、前記少なくとも一つの識別子を問いただして識別情報を生成するレシーバと、前記少なくとも一つの識別子を含む前記対象物の画像を記録するカメラ装置と、前記カメラ装置によって獲得された前記画像に沿って、コード化されたデータとして、前記レシーバからの前記識別情報をコード化して、複合データを生成する複合ジェネレータと、を有することを特徴とするシステム。

(2) 前記少なくとも一つの識別子は無線周波数（RF）識別子を有することを特徴とする上記（1）に記載のシステム。

(3) 前記少なくとも一つの識別子は生物測定的識別子を有することを特徴とする上記（1）に記載のシステム。

(4) 前記少なくとも一つの識別子はバー・コードおよびスマート・カードの少なくとも一つを有することを特徴とする上記（1）に記載のシステム。

(5) 前記レシーバは無線周波数（RF）レシーバを有することを特徴とする上記（1）に記載のシステム。

(6) 前記少なくとも一つの識別子は前記対象物および前記対象物の特徴の少なくとも一つに特有のものであることを特徴とする上記（1）に記載のシステム。

(7) 複数の識別子が前記対象物に取り付けられていることを特徴とする上記（1）に記載のシステム。

(8) 前記コード化されたデータは、添付署名および透かしの一つとして前記画像に添付されることを特徴とする上記（1）に記載のシステム。

(9) 前記レシーバは、前記少なくとも一つの識別子とは別の識別子の読み取りを前記レシーバが行うのを妨げ

るために指向性アンテナを有し、該指向性アンテナは前記カメラ装置が向いている方向にある識別子のみから無線周波数（RF）信号を受信することを特徴とする上記（1）に記載のシステム。

(10) 前記レシーバに結合し、前記対象物に向けられた前記レシーバのパルスの開始と前記レシーバによる前記パルスの受信との間の遅延時間を測定する遅延感知サブシステムを、さらに有することを特徴とする上記（1）に記載のシステム。

(11) 前記識別情報は、前記カメラ装置と前記対象物との距離と、前記カメラの焦点距離との少なくとも一つを含むことを特徴とする上記（1）に記載のシステム。

(12) 上記（1）に記載のシステムであって、前記複合ジェネレータに結合した暗号化装置をさらに有し、前記少なくとも一つの識別子と所定の情報とからの識別情報のコード化は、公開鍵および秘密鍵の一つを用いる前記複合ジェネレータから前記暗号化装置への入力であることを特徴とする上記（1）に記載のシステム。

(13) 前記カメラ装置は、ズーム・レンズ系を有し、前記ズーム・レンズ系の複数の異なるズーム設定によって複数の画像を自動的に形成することを特徴とする上記（1）に記載のシステム。

(14) 前記レシーバは該レシーバに取り付けられた識別子を有し、前記対象物の画像を前記カメラ装置が撮る際に前記レシーバの前記識別子と前記対象物の前記少なくとも一つの識別子との両方が記録されることを特徴とする上記（1）に記載のシステム。

(15) 前記少なくとも一つの識別子に対応する署名は、事前に記録されていることを特徴とする上記（1）に記載のシステム。

(16) 前記少なくとも一つの識別子は、無線周波数識別タグを有することを特徴とする上記（1）に記載のシステム。

(17) 前記画像はタイム・スタンプによりコード化されていることを特徴とする上記（1）に記載のシステム。

(18) 前記画像にタイム・スタンプを暗号化するための手段をさらに有し、前記タイム・スタンプは前記画像が前記カメラ装置によって記録された時間を表示することを特徴とする上記（1）に記載のシステム。

(19) 前記画像が前記カメラ装置によって記録された時間を感知する手段と、前記画像にタイム・スタンプを埋め込む手段と、前記タイム・スタンプを含む前記画像を暗号化する手段と、をさらに有することを特徴とする上記（1）に記載のシステム。

(20) 前記少なくとも一つの識別子は、前記少なくとも一つの識別子の变化あるいは除去のいずれの場合も前記少なくとも一つの識別子を無効にするように、耐改ざん識別子を有することを特徴とする上記（1）に記載のシステム。

(2 1) 対象物を認証する方法であって、対象物に少なくとも一つの識別子を対応づける工程と、前記少なくとも一つの識別子を問いただすことで識別情報を生成する工程と、前記少なくとも一つの識別子を含む前記対象物の画像を記録する工程と、複合データを生成するために、記録された前記画像に沿って、前記少なくとも一つの識別子に対する前記問いただしにもとづいて、前記識別情報をコード化する工程と、を有することを特徴とする方法。

(2 2) 前記少なくとも一つの識別子は無線周波数識別子を有することを特徴とする上記 (2 1) に記載の方法。

(2 3) 前記少なくとも一つの識別子は生物測定的識別子を有することを特徴とする上記 (2 1) に記載の方法。

(2 4) 前記少なくとも一つの識別子はバー・コードおよびスマート・カードの少なくとも一つを有することを特徴とする上記 (2 1) に記載の方法。

(2 5) 前記少なくとも一つの識別子は前記対象物および前記対象物の特徴の少なくとも一つに特有のものであることを特徴とする上記 (2 1) に記載の方法。

(2 6) 前記少なくとも一つの識別子は、耐改ざん識別子を有し、前記少なくとも一つの識別子の変化および除去のいずれの場合に対しても応答する前記耐改ざん識別子を無効にする工程をさらに有することを特徴とする上記 (2 1) に記載の方法。

(2 7) 対象物を認証する方法であって、前記対象物に対応した少なくとも 2 種類の情報を同時に抽出する工程と、前記抽出とともに、同時に前記少なくとも 2 種類の情報を一緒に暗号化する工程と、前記少なくとも 2 種類の情報を解読し、前記対象物の認証を確かめる工程と、を有することを特徴とする方法。

(2 8) 前記抽出する工程は、前記対象物の画像を記録する準工程と、前記対象物の固有の物理的特性を得る準工程とを有することを特徴とする上記 (2 7) に記載の方法。

(2 9) 前記画像は写真画像を有し、また前記固有の物理的特性は前記対象物の表面の地形学的測定を含むことを特徴とする上記 (2 8) に記載の方法。

(3 0) 前記画像は写真画像を有し、また前記固有の物理的特性は前記対象物の密度および重量の少なくとも一つを含むことを特徴とする上記 (2 8) に記載の方法。

(3 1) 前記密度は前記対象物の立体的空隙を明らかにすることを特徴とする上記 (3 0) に記載の方法。

(3 2) 前記画像は写真画像を有し、また前記少なくとも一つの固有の特性は前記対象物の磁性的特性をふくむことを特徴とする上記 (2 8) に記載の方法。

(3 3) 前記 2 種類の情報の一つは前記対象物の電磁気照射を有することを特徴とする上記 (2 7) に記載の方法。

(3 4) 前記 2 種類の情報の一つは、識別する情報を発

する電子タグの一つから、および外部フィールドによって促された場合に前記 2 通りの情報の一つを明らかにする受動的タグからのものであることを特徴とする上記

(2 7) に記載の方法。

(3 5) 前記 2 通りの情報の少なくとも一つは、時間順の順序で適応されることを特徴とする上記 (2 7) に記載の方法。

(3 6) 前記 2 通りの情報の少なくとも一つは、前記対象物のデジタル画像を有し、前記対象物は立体状の対象物を有することを特徴とする上記 (2 7) に記載の方法。

(3 7) 前記 2 通りの情報は、前記対象物の画像情報と前記対象物に固有に対応付けされた生物測定的情報とが含まれることを特徴とする上記 (2 7) に記載の方法。

(3 8) 前記 2 通りの情報は、前記対象物に対応付けされた無線周波数 (R F) タグであることを特徴とする上記 (2 7) に記載の方法。

(3 9) 前記 2 通りの情報は、前記対象物に対応付けされた生物測定的識別子であることを特徴とする上記 (2 7) に記載の方法。

(4 0) 前記 2 通りの情報の一つは、前記対象物に対応付けられたバー・コードおよびスマート・カードの少なくとも一つからのものであることを特徴とする上記 (2 7) に記載の方法。

(4 1) 前記 2 通りの情報の一つは、前記対象物に対応づけられた少なくとも一つの識別子からのものであり、前記少なくとも一つの識別子は耐改ざん識別子を有し、前記少なくとも一つの識別子の変化あるいは除去のいずれの場合にも応答して耐改ざん識別子を無効にする工程をさらに有することを特徴とする上記 (2 7) に記載のシステム。

【図面の簡単な説明】

【図 1】本発明の第 1 の好ましい実施形態例にもとづくシステムの模式的図である。

【図 2】本発明にもとづくシステムの概略的構成を説明するためのブロック図である。

【図 3】本発明にもとづいて、認証された画像を生成するために、対象物からの 2 種類のデータを暗号化する手順を説明するための模式図である。

【図 4】本発明にもとづいて、対象物の距離および（または）物理的測定値を得るための手段を持つカメラ装置を説明するための模式図である。

【図 5】本発明に適用される様々の双極子を持つタグの模式的平面図である。

【符号の説明】

1 0 0 システム

1 0 1 タグ

1 0 2 対象物

1 0 3 レシーバ／タグ・リーダー (R F レシーバ)

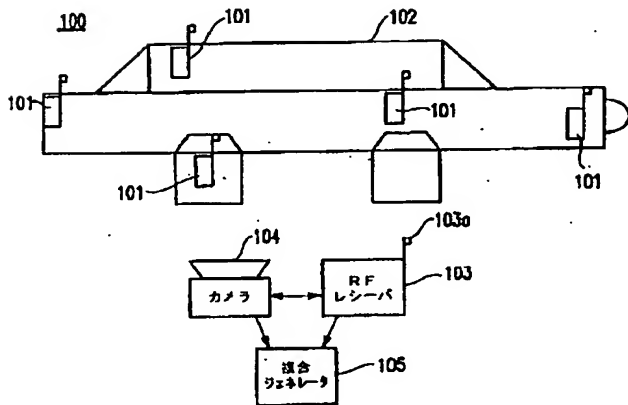
17

- 103 a アンテナ (指向性アンテナ)
 104 カメラ
 105 複合ジェネレータ
 106 遅延センサ (遅延感知サブシステム)
 107 暗号化装置
 109 タイム・スタンプ・センサ/暗号化装置
 200 システム
 300 暗号化装置
 302 カメラ画像
 304 対象物の特性
 308 暗号化装置

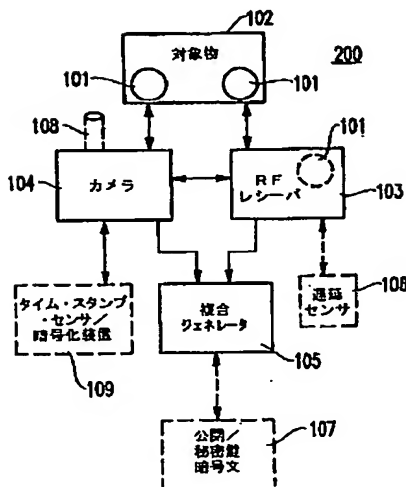
18

- 310 認証された画像
 400 デジタル・カメラ
 402 カメラのレンズ
 404 距離測定アレイ
 406 対象物
 408 電子タグ
 410 RFIDタグ・リーダ
 501 タグ
 502 双極子
 10 503 パッケージング/ハウジング

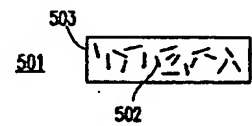
【図 1】



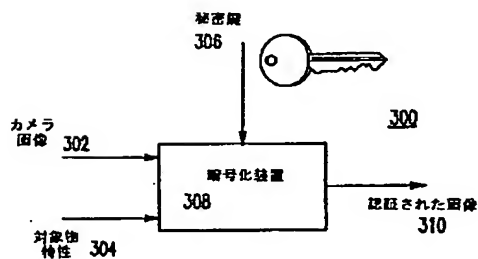
【図 2】



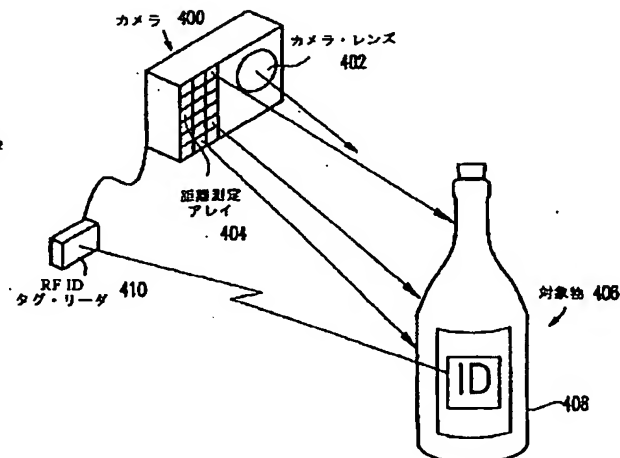
【図 5】



【図 3】



【図 4】



フロントページの続き

(51) Int. Cl.	識別記号	F I	テーマコード (参考)
G 0 6 K 19/07		G 0 6 F 15/21	Z
G 0 9 C 1/00	6 4 0	G 0 6 K 19/00	H
H 0 4 N 1/387			
(72) 発明者 ティモシー・ジョセフ・チャイナー アメリカ合衆国10541 ニューヨーク州、 マホバック、 バレット・ヒル・ロード 161		(72) 発明者 アレンドロ・ガブリエル・スクロット アメリカ合衆国10011 ニューヨーク州、 ニューヨーク、 ウェスト・トゥエルフ ス・ストリート 175 アpartment 9ービー	
(72) 発明者 クラウド・エー・グリーンガード アメリカ合衆国10514 ニューヨーク州、 チャパックア、 ジェフリー・レーン 40		(72) 発明者 チャールズ・ピー・トッレサー アメリカ合衆国10543 ニューヨーク州、 ママロネック、 ウェスト・ボストン、 ポスト・ロード 953 アpartment 2ケー	
(72) 発明者 ポール・アンドリュウ・モスコウツ アメリカ合衆国10598 ニューヨーク州、 ヨークタウン・ハイツ、 ハンタープロ ック・ロード 2015		(72) 発明者 ロバート・ヤコブ・ヴォンガトフェルド アメリカ合衆国10025 ニューヨーク州、 ニューヨーク、 ウェスト・ハンドレッ ドフィフティーンズ・ストリート 600 アpartment 113	